IMPLEMENTASI DAN ANALISIS *VIDEO STEGANOGRAFI* DENGAN FORMAT *VIDEO AVI* BERBASIS LSB (*LEAST SIGNIFICANT BIT*) DAN SSB-4 (*SYSTEM OF STEGANOGRAPHY USING BIT 4*)

IMPLEMENTATION AND ANALYSIS OF STEGANOGRAPHY AVI VIDEO BASED ON LSB (LEAST SIGNIFICANT BIT) AND SSB-4 (SYSTEM OF STEGANOGRAPHY USING BIT 4)

Farisah Qisthina Rekamasanti[1], Dr. Ir. Bambang Hidayat,DEA[2], I Nyoman Apraz Ramatryana, ST., MT.[3]
[1,2,3]Electrical Engineering Faculty – Telkom University
Jl.Telekomunikasi No.1, Dayeuh Kolot, Bandung 40257 Indonesia
farisahqisthina@yahoo.com[1], avenir.telkom@gmail.com[2], ramatryana@gmail.com[3]

ABSTRAK

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain pengirim dan penerima, tidak ada yang dapat mengetahui atau menyadari bahwa ada suatu pesan rahasia. Kata "steganografi" berasal dari bahasa Yunani *steganos*, yang artinya "tersembunyi atau terselubung", dan *graphein*, "menulis". Pesan yang tertulis ini merupakan tulisan yang menyelubungi atau menutupi[1]

Penyisipan informasi yang digunakan pada tugas akhir ini menggunakan teknik *steganography video* serta penerapannya ke dalam video berformat AVI dengan metode *Least Significant Bit* (LSB) *dan System of Steganography using Bit 4* (SSB-4). Penyisipan informasi pada video menggunakan *Pseudo Random Number Generator (PRNG)* sebagai metode pengacakan. Hasil keluaran *PRNG* akan menentukan metode penyisipan informasi yang akan dipakai. Pada metode LSB, penyisipan informasi akan menggantikan bit LSB dari video asli. Sedangkan pada metode SSB-4, penyisipan bit informasi akan mengganti bit ke 4 dari video asli.

Dari hasil penelitian, metoda yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah, bit yang paling kanan (LSB) atau pada bit keempat (SSB-4). Pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) dan gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Aplikasi ini dibuat dengan bahasa pemrograman MATLAB.

Kata Kunci : Stego, Steganografi, LSB, SSB-4

ABSTRACT

Steganography is a technology to insert a hidden message in a way that only sender and receiver can see the message. The word "steganography" comes from Greek word "steganos" which means hidden, and "Graphein" which means write [1].

Information insertion is used in this final project using video steganography technique and the implementation to AVI format video using LSB and SSB method. This information insertion is using PRNG as a method of randomization. The outcome PRNG (Pseudo Random Number Generator) will decide which method will be used. In LSB method, Information insertion will replace the least significant Bit of the original video. -4 method However, in SSB-4, information insertion will replace the fourth bit of the original video.

In the result, different method is used to insert a hidden message in digital media. The message can be hidden by using a method to insert in the lowest bit, LSB(Least Significant Bit), or in the fourth bit (SSB-4). In 24 bit bitmap file, every pixel in the picture consist of three different color, Red, Green, Blue (RGB). Each pixel is form by 8 bit(byte) from 0 to 255 in biner format 00000000 to 11111111. This application is made with matlab.

Keywords: *Stego, steganography, LSB, SSB-4*

PENDAHULUAN

Steganografi memberikan solusi untuk penyembunyian pesan yang sering digunakan dalam proses pengiriman data. Steganografi adalah teknik menyisipkan pesan kedalam suatu media, dimana pesan rahasia yang akan dikirimkan tidak diubah bentuknya, melainkan disisipkan pada sebuah media lain (cover) yang digunakan dalam kehidupan sehari-hari. Media baru yang telah disisipi pesan rahasia (stego) kemudian dikirim kepada penerima tanpa menimbulkan kecurigaan dari pihak luar, karena perbedaan dari media asli (cover) dengan media yang telah disisipi pesan rahasia (stego) tidak dapat disadari secara langsung oleh manusia. Steganografi pada masa kini dilakukan pada media digital berupa citra, audio, maupun video.

Least Significant Bit (LSB) dan *System of Steganography using Bit 4 (SSB-4)* merupakan teknik penyembunyian data yang bekerja pada domain spatial atau waktu. Pengubahan LSB dan SSB-4 pada gambar, suara, dan video yang tidak terkompresi sulit diketahui secara kasat mata. Metode ini memanfaatkan ketidakmampuan mata manusia dalam menemukan perbedaan antara citra asli dengan yang sudah dimasukkan pesan tersebunyi (stego). Dengan kemampuan metode LSB dan SSB-4 tersebut, penulis menerapkannya sebagai metode menyembunyikan pesan.

1. DASAR TEORI

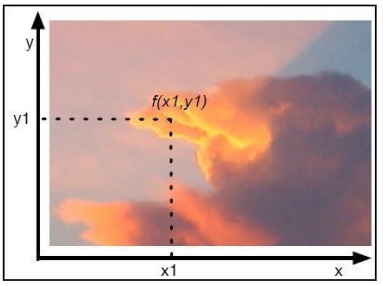
1.1 Steganografi

Steganografi berasal dari bahasa Yunani *steganos* yang artinya "tersembunyi" dan *graphein* yang artinya "menulis". Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia[2]. Dalam pengimplemantasiannya, steganografi menggunakan berbagai macam objek multimedia baik sebagai *hos t*maupun *message* seperti *file* citra, audio, teks atau video.

1.2 Citra Digital

Citra digital dapat didefinisikan sebagai fungsi dua variabel, *f(x,y)*, dimana *x* dan *y* adalah koordinat spasial dan nilai *f(x,y)* adalah intensitas citra pada koordinat tersebut. Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red, Green, Blue* - RGB). Dan berikut adalah gambar citra digital sebagai matriks dua dimensi dan ilustrasi citra digital

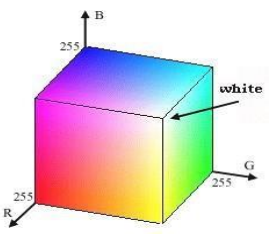
.Gambar 1.1 Citra Digital sebagai matriks dua dimensi [3]



Gambar 1.2 Ilustrasi Citra Digital [3]

1.3 RGB (Red, Green, Blue)

Citra berwarna yang selama ini biasa kita kenal umumnya memiliki ruang warna RGB. Ruang warna RGB dapat divisualisasikan sebagai sebuah kubus seperti pada gambar 1.3, dengan tiga sumbunya yang mewakili komponen warna merah (*red*) *R*, hijau (*green*) *G* dan biru (*blue*) *B*. Salah satu pojok alas kubus ini menyatakan warna hitam ketika *R = G = B = 0*, sedangkan pojok atasnya yang berlawanan menyatakan warna putih ketika *R = G = B = 255* (untuk sistem warna 8 bit bagi 24 setiap komponennya). RGB sering digunakan didalam sebagian besar aplikasi komputer karena dengan ruang warna ini, tidak diperlukan transformasi untuk menampilkan informasi di layar monitor. Alasan diatas juga menyebabkan RGB banyak dimanfaatkan sebagai ruang warna dasar bagi sebagian besar aplikasi.

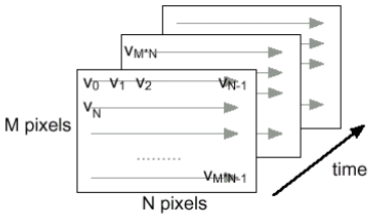


Gambar 1.3 Ruang warna RGB [3]

1.4 Video Digital

Video Digital adalah jenis sistem video recording yang bekerja menggunakan sistem digital dibandingkan dengan analog dalam hal representasi videonya. Digital video memiliki banyak kelebihan dibandingkan analog video, yang paling penting adalah ketepatan yang tinggi dalam proses transmisi (high fidelity) dibandingkan dengan sinyal analog. Pada sinyal analog, saat penerimaan akhir transmisi akan sulit membedakan antara sinyal asli dan noise yang mungkin diperkenalkan selama transmisi. Dengan transmisi yang diulang-ulang maka akumulasi noise tidak dapat dihindari. Lain halnya dengan sinyal digital yang dapat membedakan antara sinyal asli dan noise. Sinyal digital juga dapat ditransmisikan berulang-ulang sebanyak yang kita inginkan tanpa mempengaruhi kualitasnya.Video digital disimpan dalam media penyimpanan contohnya magnetic / optical disk.

Video Digital tersusun atas serangkaian frame yang ditampilkan dengan kecepatan tertentu (frame/detik). Jika laju frame cukup tinggi, maka mata manusia akan melihat sebagai rangkaian kontinyu. Setiap frame merupakan gambar atau citra digital. Sutau citra digital direpresentasikan dengan sebuah matriks yang masing-masing elemennya memperesentasikan nilai intensitas atau kedalaman warna..



Gambar 1.4 Ilustrasi tiga dimensi video [3]

1.5 Audio Video Interleave (AVI)

AVI merupakan format file penyimpan data-data multimedia. AVI diperkenalkan pertama kali oleh Microsoft pada bulan November 1992 sebagai bagian dari teknologi video dalam flatform Microsoft Windows. Format file AVI dapat menyimpan data video dan audio dan dapat memainkan kedua jenis data tadi secara bersamaan. AVI memiliki jenis *codec* yang berbeda-beda, seperti halnya MPEG yang memiliki jenis berbeda- beda (MPEG1, MPEG2, MPEG4). Dalam Tugas Akhir ini memakai video jenis AVI *uncompressed* atau disebut juga AVI full frames. Suatu file multimedia dengan format AVI *uncompressed* memiliki informasi frame-frame gambar yang disimpan dengan menggunakan format Bitmap tiga layer warna 8 bit, jadi untuk satu pixel data bitmap akan disimpan dalam wadah berukuran 24 bit. Format file AVI termasuk salah satu format yang menggunakan metaformat RIFF (*Resource Interchange File Format*) yang membagi data ke dalam bagian- bagian atau blok-blok yang disebut *"chunck"*. Setiap chunck diidentifikasi dengan tag-tag tertentu seperti pada struktur file berformat RIFF berikut, dimana masing-masing tag memiliki kode unik empat bytes.

1.6 LSB (Least Significant Bit)

LSB (Least Significant Bit) Coding. Metoda ini merupakan metoda yang sederhana. Metoda ini akan mengubah nilai LSB (*Least Significant Bit*) komponen luminansi atau warna menjadi *bit* yang bersesuai dengan *bit* label yang akan disembunyikan. Memang metoda ini akan menghasilkan video rekontruksi yang sangat mirip dengan aslinya, karena hanya mengubah nilai *bit* terakhir dari data. Metoda ini paling mudah diserang, karena bila orang lain tahu maka tinggal membalikkan nilai dari LSB-nya maka data label akan hilang seluruhnya.

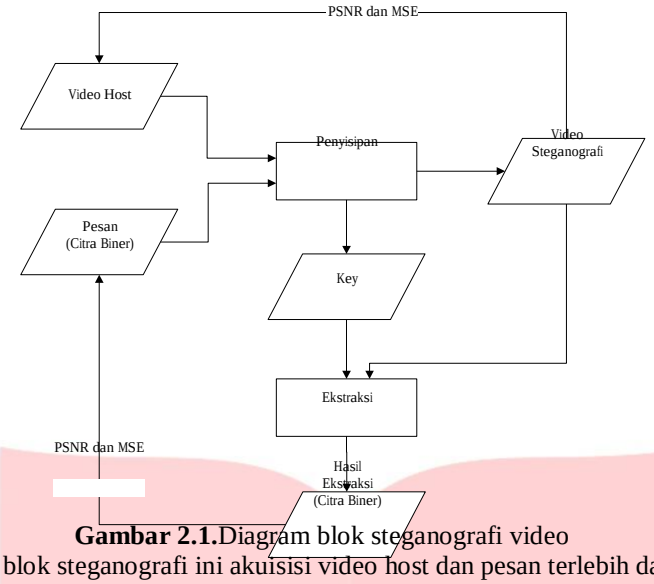
1.7 SSB-4 (System of Steganograph using Bit-4)

Pada teknik SSB-4 ini dikembangkan oleh J.M.Rodrigues, J.R.Rios dan W.Puech. Dalam image RGB 24bit, variasi-variasi kecil dalam nilai channel color tidak nampak oleh mata manusia. Metode yang diajukan dapat diaplikasikan pada citra yang disimpan dalam setiap tipe format file yang ada, selama menggunakan 8 bit per color dan menggunakan kompresi lossless. Bit ke 4 dari citra cover akan digantikan oleh bit pesan dan memodifikasi bit-bit reminder (1,2,3 dan 5). Ukuran citra pesan harus lebih kecil dari citra cover-nya. Berikut ini adalah contoh metode SSB-4 dengan menggunakan citra pesan berupa citra biner dan citra cover berupa Grayscale.

2. PEMBAHASAN

2.1 Deskripsi Sistem Video Steganografi

Dalam implementasi dan perancangan sistem ini akan di bangun sistem yang mensimulasikan video steganografi dengan metode LSB, SSB-4, dan gabungan LSB dan SSB-4. Simulasi sistem *video steganography* pada tugas akhir ini terdiri atas bagian *embedding* (penyisipan) dan bagian ekstraksi. Dan berikut gambarnya:



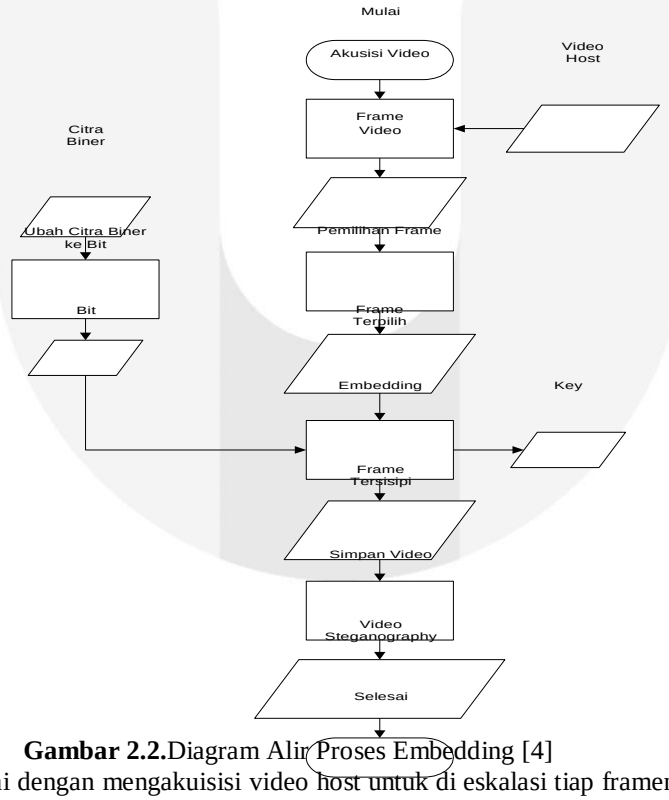
Gambar 2.1. Diagram blok steganografi video

Proses pertama diagram blok steganografi ini akuisisi video host dan pesan terlebih dahulu, kemudian proses penyisipan dilakukan setelah pesan dikonversi kedalam citra biner. Penyisipan pesan ke dalam video host memberi keluaran sebagai video steganografi. Proses penyisipan melibatkan key sebagai penentu lokasi bit penyisipan.

Kemudian proses ekstraksi dilakukan dengan cara memanggil video steganografi dan menentukan lokasi bit penyisipan dari key yang di simpan tersebut. Penentuan PSNR dan MSE penyisipan dilakukan dengan cara membandingkan hasil video steganografi dengan video host. Penentuan nilai PSNR dan MSE ekstraksi dilakukan dengan membandingkan hasil pesan ekstraksi dengan pesan asli.

2.2 Proses Embedding

Bagian ini akan dibahas teknik steganografi yang akan menggunakan metode LSB dan SSB-4 untuk proses penyisipan stegano tersebut. Diagram alir proses penyisipan (embedding) sistem video steganografi dapat dilihat pada gambar di bawah ini :



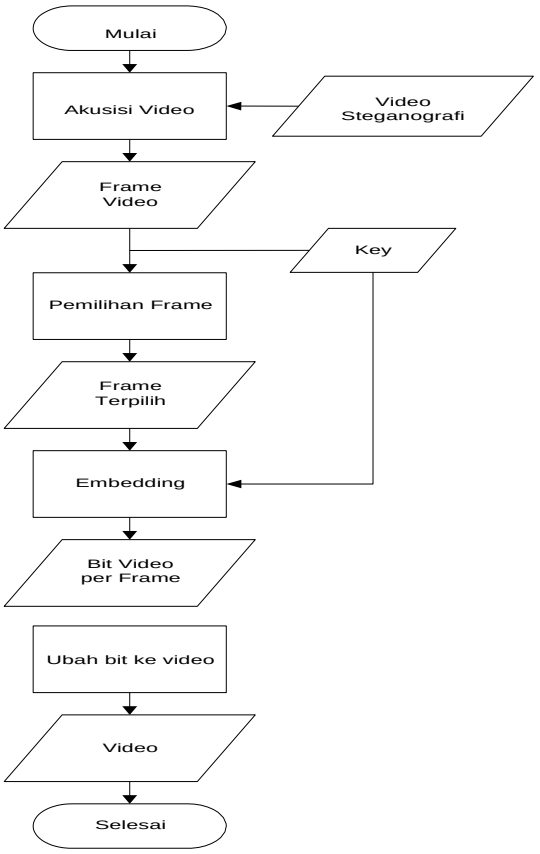
Gambar 2.2. Diagram Alir Proses Embedding [4]

Proses penyisipan dimulai dengan mengakuisisi video host untuk di eskalasi tiap framenya. Satu buah frame akan dipilih untuk proses embedding atau penyisipan. Proses embedding dimulai dengan menyisipkan nilai bit

dari image yang sudah dikonversi kedalam citra biner. Proses embeding dilakukan tiap frame untuk seluruh frame video. Kemudian kumpulan embbeded frame disimpan sebagai video steganografi.

2.3 Proses Ekstraksi

Pada bagian ini akan dibahas teknik pengekstraksian video steganografi. Pada proses ekstraksi yang dibutuhkan sebuah video steganografi yang telah disisipkan citra biner dan key. Diagram alir proses ekstraksi sistem video steganografi dapat dilihat pada gambar berikut:



Gambar 2.3 diagram alir proses ekstraksi [5]

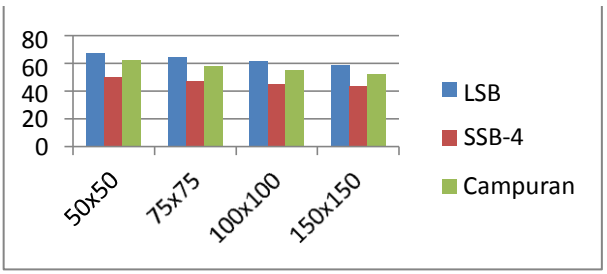
Proses ekstraksi dimulai dengan mengakuisisi video steganografi untuk dipisahkan tiap masing-masing framenya. Kemudian key yang telah disimpan dipanggil kembali untuk menentukan posisi penyisipan bit pada frame tersebut. Pemanggilan bit tersisip dilakukan pada tiap frame berdasar key. Bit yang diperoleh direkonstruksi kembali menjadi sebuah file citra.

3. HASIL PENGUJIAN

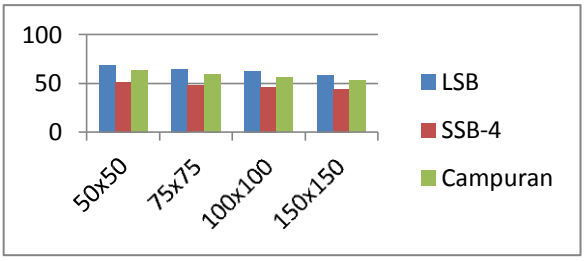
3.1 Hasil Analisis Pengujian Sistem

3.1.1 Perbandingan PSNR ketiga Logo

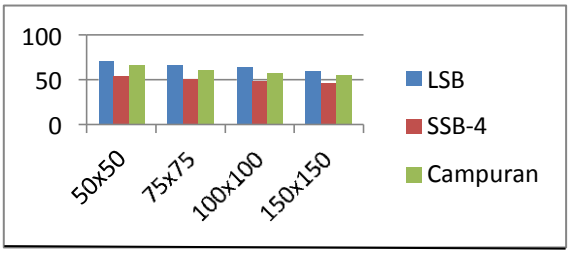
Untuk nilai PSNR, dimana persamaan PSNR didapat dari nilai MSE. Sehingga apabila MSE semakin besar maka nilai PSNR akan semakin kecil..



Gambar 3.1 PSNR Logo BUNGA



Gambar 3.2 PSNR Logo QISTHI

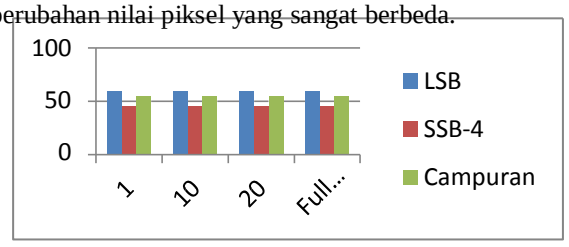


Gambar 3.3 PSNR Logo TEL-U

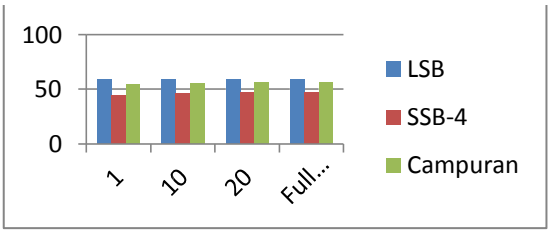
Berdasarkan gambar 3.1, 3.2, dan 3.3, didapatkan hasil bahwa nilai PSNR terbesar adalah pada metode LSB dikarenakan metode LSB merupakan metode yang memiliki error paling kecil karena hanya mengubah nilai LSB sehingga perubahan piksel yang mungkin paling besar adalah 1 intensitas piksel. Sedangkan untuk SSB-4 memiliki perubahan nilai terbesar 8 dan bervariasi sesuai proses reminder. Untuk metode campuran yang merupakan gabungan antara LSB dan SSB-4 akan memiliki nilai PSNR yang terbesar kedua. Pada pengujian ini hanya memandang nilai MSE dan PSNR antara video host dan video steganografi dikarenakan untuk MSE dan PSNR logo hasil ekstraksi terhadap Logo asli akan selalu memiliki MSE bernilai nol atau sama sekali tidak ada error dikarenakan belum terdapat gangguan pada video steganografi. Semakin kecil resolusi logo maka nilai PSNR akan semakin besar hal ini dikarenakan nilai piksel yang berubah akan semakin sedikit yang menyebabkan nilai MSE semakin kecil.

3.1.2 Pengujian pengaruh banyak frame penyisipan stego

Berdasarkan Tabel, untuk ukuran frame video yang sama yaitu 1280x768 namun disisipkan logo dengan banyak frame yang berbeda akan menyebabkan nilai MSE akan semakin besar untuk video gelap. Untuk video terang besar mse rata-rata sama berarti mse untuk banyak frame yang semakin banyak akan tetap memiliki rata-rata mse yang sama. Hal ini dikarenakan setiap frame disisipkan 1 logo yang sama. Akan berbeda apabila setiap frame yang berdekatan memiliki perubahan nilai piksel yang sangat berbeda.



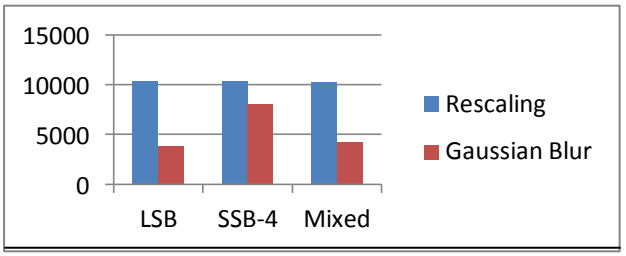
Gambar 3.4 PSNR banyak frame video Terang



Gambar 3.5 PSNR banyak frame video Gelap

3.1.3 Pengaruh ketahanan sistem steganografi saat diberi gangguan

Berikut ini adalah data dan grafik yang memperlihatkan pengaruh ketahanan sistem steganografi saat diberi Rescaling dan Gaussian Blur.



Gambar 3.6 rata-rata MSE tiap jenis gangguan

Berdasarkan gambar 3.6 didapatkan hasil bahwa nilai MSE hasil ekstraksi yang paling kecil adalah pada metode SSB-4 dikarenakan metode SSB-4 merupakan metode yang lebih robust karena perubahan nilai pikselnya lebih besar disbanding metode lain.

4. KESIMPULAN

Berdasarkan hasil implementasi, pengujian, dan analisis yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut :

1. Perancangan suatu sistem video steganografi dengan metode LSB lebih *robust* karena memiliki nilai PSNR paling tinggi sebesar 70.57 dibandingkan dengan metode SSB-4 dengan nilai 53.25 ataupun dengan menggunakan metode penggabungan antara SSB-4 dan LSB yang menggunakan pengacakan PRNG yang menghasilkan nilai PSNR sebesar 65.61.
2. Semakin besar resolusi frame video *host* akan memerlukan waktu komputasi yang lebih lama pada saat proses penyisipan maupun ekstraksi. Selain itu semakin besar resolusi frame video *host* member nilai PSNR yang lebih besar pula pada saat proses penyisipan.
3. Semakin besar resolusi logo akan memerlukan waktu komputasi yang lebih lama pada saat proses penyisipan maupun ekstraksi. Namun semakin kecil resolusi logo akan memberikan nilai PSNR yang semakin besar pula pada saat proses penyisipan.
4. Jumlah frame video *host* yang disisipi tidak berpengaruh secara signifikan terhadap nilai PSNR. Semakin banyak jumlah frame video yang disisipi hanya akan berpengaruh pada waktu komputasi yang semakin lama.
5. Intensitas cahaya pada video berpengaruh pada kontras cahaya. Semakin kecil kontrasnya akan membuat nilai bit hitam menjadi semakin kecil yang membuat banyak bit-bit yang nilainya berdekatan dengan bit hitam tersebut, sehingga video dengan intensitas cahaya rendah memiliki kemungkinan *error* lebih besar daripada video dengan intensitas cahaya yang tinggi,
6. Semakin besar nilai konstanta *rescalling* semakin memberi respon baik dengan indikasi makin menurunya nilai MSE. Hal ini berlaku baik pada metode LSB,SSB-4, maupun metode campuran.
7. Semakin besar nilai konstanta *noise* pada Gaussian *Blur* memberi respon semakin buruk dengan indikasi makin membesarnya nilai MSE. Hal ini berlaku baik pada metode LSB,SSB-4, maupun metode campuran..

5. SARAN

Saran yang dapat digunakan untuk perkembangan penelitian Tugas Akhir selanjutnya, yaitu :

1. Mengubah citra cover dengan format cover lain (MPEG, Blueray,dll) untuk dapat disisipkan berkas data *stego*.
2. Mencoba mengembangkan program dengan orientasi implementasi pada kasus aktual dan rieal time, misal pada android
3. Aplikasi ini perlu dikembangkan lagi agar dapat menyisipkan berkas data kepemilikan dalam ukuran yang lebih besar dan format steganografi lain misal *barcode*, *voice*, dll.

6. REFERENSI

[1] Eriel Mar, **"Implementasi dan Analisis Video Steganografi dengan Format Video MPEG Berbasis Wavelet Transform"**, Sekolah Tinggi Teknologi Telkom Bandung, 2009.
[2] Mohanti SP. 1999, **Digital Steganografi :** A Tutorial Riview. University of South Florida.
[3] Cahyana ; T. Basarudin dan Danang Jaya. 2007. **Teknik *Steganografi* Citra berbasis SVD**. National Conference on Computer Science & Information Technology 2007. Januari 29-30,2007.

[4] Fery Sinambela, Ranto Pramono, dan Krisna Adirama. 2006. **"Teknologi *Steganografi* yang Kuat pada Video MPEG".** Institut Teknologi Bandung, Bandung.
[5] Harry Kurniawan, **"Peningkatan Robustness Citra berwatermark dengan Region Menggunakan Metode LSB"**, Sekolah Tinggi Teknologi Telkom Bandung, 2008.